Strategy Research Project

ORGANIZATION OF DOD COMPUTER NETWORK DEFENSE, EXPLOITATION, AND ATTACK FORCES

BY

LIEUTENANT COLONEL KRAIG HANSON
United States Air Force

USAWC CLASS OF 2009

U.S. Army War College, Carlisle Barracks, PA 17013-5050

The U.S. Army War College is accredited by the Commission on Higher Education of the Middle State Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
12-03-2009	Strategy Research Project	

4. TITLE AND SUBTITLE

Organization of DoD Computer Network Defense, Exploitation, and Attack Forces

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Lieutenant Colonel Kraig Hanson

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Colonel Kevin Smith
Department of Military Strategy, Planning, and Operations

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Army War College
122 Forbes Avenue
Carlisle, PA 17013

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution A: Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The Department of Defense (DoD) faces many challenges in the world of computer networks and systems. Technical skills used to exploit adversary networks and systems for intelligence purposes can also be used to attack adversary networks and systems. In the likelihood that exploitation is much more common than attack, technicians performing exploitation will gain much experience in their work. Because of this, these same technicians should also perform attack functions, as opposed to having separate forces. With respect to computer network defense, there are multiple DoD entities with varying interests and this has led to complicated organizational relationships. Realizing that computer network defense authority emanates from the Secretary of Defense, a simpler structure is to delegate his authority to a DoD entity and allow this entity to act on his behalf. These changes, should they be implemented, would continue DoD progress in cyberspace, allowing it to better protect U.S. security.
.

15. SUBJECT TERMS
CND, CNE, CAN, JFCC-NW, JTF-GNO

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. TELEPHONE NUMBER** *(include area code)*
UNCLASSIFED	UNCLASSIFED	UNCLASSIFED	UNLIMITED	28	

USAWC STRATEGY RESEARCH PROJECT

ORGANIZATION OF DOD COMPUTER NETWORK DEFENSE, EXPLOITATION, AND ATTACK FORCES

by

Lieutenant Colonel Kraig Hanson
United States Air Force

Colonel Kevin Smith
Project Adviser

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR: Lieutenant Colonel Kraig Hanson

TITLE: Organization of DoD Computer Network Defense, Exploitation, and Attack Forces

FORMAT: Strategy Research Project

DATE: 12 March 2009 WORD COUNT: 5,663 PAGES: 28

KEY TERMS: CND, CNE, CNA, JFCC-NW, JTF-GNO

CLASSIFICATION: Unclassified

The Department of Defense (DoD) faces many challenges in the world of computer networks and systems. Technical skills used to exploit adversary networks and systems for intelligence purposes can also be used to attack adversary networks and systems. In the likelihood that exploitation is much more common than attack, technicians performing exploitation will gain much experience in their work. Because of this, these same technicians should also perform attack functions, as opposed to having separate forces. With respect to computer network defense, there are multiple DoD entities with varying interests and this has led to complicated organizational relationships. Realizing that computer network defense authority emanates from the Secretary of Defense, a simpler structure is to delegate his authority to a DoD entity and allow this entity to act on his behalf. These changes, should they be implemented, would continue DoD progress in cyberspace, allowing it to better protect U.S. security.

ORGANIZATION OF DOD COMPUTER NETWORK DEFENSE, EXPLOITATION, AND ATTACK FORCES

Whether in sports, business, or government, adversaries seek to gain advantage over their opponents. As the Department of Defense (DoD) has formidable conventional power, adversaries often avoid conventional conflict. With the advent of the Internet and other interconnected networks, adversaries suddenly have the potential to access Department of Defense information that would formerly have required insider access to obtain. Further, they may be able to access DoD systems, such as e-mail and logistics systems, to influence DoD operations. Much of the activity to gain access can be low risk because it is done remotely and perpetrators can employ many concealment techniques. DoD efforts to prevent adversary access to DoD systems and information include the field of computer network defense (CND). In addition, the DoD has computer network exploitation (CNE), and computer network attack (CNA) capabilities it employs against adversaries. As will be shown, the CNE and CNA fields are closely related and should be organized together. On the other hand, as CND forces exist throughout the DoD, the DoD has created complicated command and control (C2) relationships that can be greatly simplified by making use of the power of the Secretary of Defense (SECDEF).

Background

Although the DoD consistently states it is under constant cyber attack, like many companies the DoD rarely discloses specific breaches of computer security and theft of information. Investigative journalists have tracked down and reported alleged details of some of these attacks, such as those detailed in the 2005 *Time* article by Elaine

Shannon, *The Invasion of the Chinese Cyberspies (And the Man Who Tried to Stop Them*. In this article, Shannon details the volume of information stolen from across the DoD and other entities such as the World Bank. Unnamed government analysts rank the group behind these attacks “among the most pervasive cyberespionage threats that U.S. computer networks have ever faced.”[1] Shannon's sources attribute the technical source of the attacks as originating from behind network routers in China. However, despite the title of the article, sources would only speculate that the group is Chinese government sponsored because of the sophistication and magnitude of the effort. Whether state sponsored or not, the lesson is that the DoD faces determined adversaries with the technical means to access our networks and exfiltrate information.

Clearly, the DoD needs effective security and counterintelligence capabilities to manage the threat to its networks. All DoD personnel with access to networks have a role to play in security. End users need to abide by the rules and, for instance, not open attachments from un-trusted sources that may compromise information systems. Administrators must configure systems in accordance with security rules. Network defenders must analyze intrusion alarms, investigate, and report incidents. Counterintelligence and law-enforcement officers must screen these incidents for trends, categorize them, and prioritize them for investigation, exploitation, or prosecution. Given the magnitude of the effort, and the fact that all DoD personnel and organizations are affected, there are related organizational and authority issues. As the Services procure and operate installation networks mostly independently, should they also handle CND mostly independently? Alternatively, since service forces ultimately exist for assignment to or support of combatant commands, is a joint approach more

appropriate? How should the DoD CND relate to other departments and entities of the USG?

But the DoD is not just on the defensive. It also has capabilities in the form of intelligence gathering and, if necessary, attack. Traditional areas of intelligence and operations that are now included in the cyber realm are still very relevant today, such as intercepting and jamming signals and conventional attacks on infrastructure. However, there are newer aspects of the cyber realm, such as using computer networks to "hack" into target systems and extract information or conduct an attack. The DoD grew its force to conduct these missions. But given the infancy of the field, is it properly organized? Where should these specialists work, in a central agency, out in the field, or a mixture of both? How should these forces be assigned to combatant commands?

According to the DoD, cyberspace is "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[2] Most readers are probably familiar with some of the general-purpose sub-domains of cyberspace such as the Internet, the DoD Non-Secure Internet Protocol Router Network (NIPRNET), the DoD Secret Internet Protocol Router Network (SIPRNET), and the Defense Switched Network (DSN). Less familiar may be more specialized sub-domains such as tactical data links used by military forces to, among other things, exchange friendly and enemy positional data. Just as DoD cyberspace can be divided into sub-domains, so can global cyberspace.

Several key sub-domains of cyberspace include DoD, U.S. non-DoD, and foreign cyberspace. DoD cyberspace refers to that portion of cyberspace with DoD

infrastructure, such as the NIPRNET. In all three sub-domains the DoD has an interest in strategic communications, effectively conveying its messages to audiences around the world. In addition to this overarching interest, the DoD has separate interests in each of the sub-domains. DoD interests in DoD and foreign cyberspace are straightforward. Within DoD cyberspace, DoD responsibilities are information assurance and counterintelligence. In other words, the DoD desires to protect its networks, detect intrusions, learn from the techniques employed by the intruders, and perform counterintelligence. Within the foreign sub-domain, DoD and other members of the Intelligence Community are naturally interested in collecting intelligence. The DoD also has an interest in network attack as stated in the mission of U.S. Strategic Command's (USSTRATCOM) Joint Functional Component Command for Network Warfare (JFCC-NW) which reads "plans, and when directed, executes operations in and through cyberspace to assure U.S. and allied freedom of action, denying adversaries' freedom of action, and enabling effects beyond the cyber domain."[3] DoD interests in U.S. non-DoD cyberspace, however, are less clear and warrant more detailed explanation.

The DoD is but one of several entities with interests in U.S. non-DoD cyberspace. With respect to defending this sub-domain, it is interesting to note that according to The National Strategy to Secure Cyberspace, "in general, the private sector is best equipped and structured to respond to an evolving cyber threat."[4] In other words, just as individuals and businesses can invest in their own physical security with guards, alarms, locks, and the like, they can also invest in cyber security. However, with respect to the U.S. Government (USG), several federal departments have responsibilities, including the Department of Homeland Security (DHS), the Department

of Justice, and the DoD. The DHS National Cyber Security Division (NCSD) "works collaboratively with public, private, and international entities to secure cyberspace."[5] The NCSD oversees the National Cyber Response System including the National Cyber Response Coordination Group, of which the DoD is one of 13 federal agency members. The FBI leads the investigation and prosecution of cyber-crime.[6] Just as other USG entities have defined their roles in U.S. non-DoD cyberspace, so has the DoD.

The DoD has two roles in U.S. non-DoD cyberspace stemming from the same roles it has in non-cyberspace, defense of the nation and national incident response.[7] The National Military Strategy for Cyberspace Operations states with respect to defense of the nation, "DoD will execute the full range of military operations in and through cyberspace to defeat, dissuade, and deter threats against U.S. interests."[8] It also states with respect to national incident response DoD will provide military support to civil authorities. There can be tensions between the defense mission and the support mission, such as a choice between quickly terminating an attack versus collecting evidence for prosecution. The Strategy for Cyberspace Operations addresses this issue by saying defense of vital interests take precedence over other missions.

Organization of Computer Network Exploitation and Attack Forces

As the cyber domain intersects with the physical world, there are a variety of ways to attack it. For instance, if you want to deny an enemy the use of their more secure, internal e-mail system and hopefully divert them to a less secure, external e-mail system you can physically destroy their e-mail servers using conventional military forces. Unlike physical destruction, covert remote access is much more flexible. With covert remote access, agents can collect information as well as conduct offensive

operations such as editing or planting information or denying use of information. This distinction is at the heart of perceiving the cyber domain as a separate domain; it is possible to operate completely within cyberspace in ways different from other domains.

There are several methods of collecting information in cyberspace, most notably open-source intelligence (OSINT) as well as traditional and CNE types of signals intelligence (SIGINT). OSINT is gathering information from publically available sources, such as an extremist web site, analyzing it, and producing intelligence. Traditional SIGINT is a broad field that, for instance, involves obtaining a signal by intercepting transmissions or tapping cables, decrypting it, processing it, and hearing or reading raw private communications. Traditional SIGINT is the historical role of the National Security Agency (NSA). CNE refers to secretly infiltrating a network or information system and obtaining private information. Technical expertise is essential for all collection disciplines. OSINT may require, for instance, automation to conduct searches as well as obscure the identity of collectors, because hundreds of government agents reading a particular forum might cause an unwanted change in behavior of the participants. Traditional SIGINT and CNE differ in that the former requires expertise in signal processing and cryptography while the latter requires network and computer intrusion expertise. This intrusion expertise required for CNE relates to the similar expertise required for CNA.

In addition to operating in cyberspace by gathering information, the DoD also operates by conducting CNA. With respect to both intelligence and attack forces that operate within the cyber domain, the ability to collect private information and the ability to affect information and systems are both greatly enhanced by privileged system

access, access that outsiders would not normally have. Note that enhanced access enables both information gathering as well as attack. For example, if an agent can remotely retrieve a user's private e-mail, he most likely has access to modify or disable e-mail. In order to conduct such an operation, an agent must reconnoiter target systems, evade intrusion detection systems, compromise target system defenses, establish covert communications, conceal the intrusion, and retain system access while protecting vital access techniques from discovery. Once those steps are completed an agent can collect information or conduct an attack. Clearly, the more difficult phase of the operation is gaining access as opposed to exploiting it. Because gaining access is specialized and crucial to both intelligence and attack, intelligence and attack forces are discussed concurrently. Although little public information on specific USG foreign computer network infiltration capabilities exists, it is possible to make general recommendations on organization of DoD CNE/CNA forces based on high-level USG organization, DoD doctrine, and analysis of functions.

With respect to organization of cyber intelligence and attack forces, there are many alternatives. Agents need expertise in many areas for successful operations. As discussed above, gaining privileged access is one area of expertise. Others include target system expertise, such as the ability to retrieve or plant e-mails; information expertise, such as the ability to search through information relative to an operation; and effects expertise, the ability to translate operational goals into concrete attacks. The first two roles, gaining access and expertly manipulating a system, are common across many potential operations. Agents in these roles are directly accessing target systems. The last two roles direct the activities of the first two. The information expert is the

detective or analyst. This expert knows which e-mail accounts are important and what key words to search with. The expertise in effects is provided by an offensive planner, such as a combatant command planner.

Although it is possible for one individual to perform all of these roles, it is more likely individuals will specialize, and this is what we frequently find today. The first two roles become the technicians, performing the exacting work of gaining access and manipulating systems, as directed by the intelligence analyst and the operations planner. There are many alternative organizations of the technicians. In current practice, the 2008 Unified Command Plan, which assigns missions and areas of responsibility to commanders, gives a cyberspace mission to USSTRATCOM which it executes through its subordinate commands, JFCC-NW and Joint Task Force for Global Network Operations (JTF-GNO). [9] Given the global nature of cyberspace, this coincides with other global missions given to USSTRATCOM and executed through subordinate commands, such as Joint Functional Component Command for Global Strike and Joint Functional Component Command for Space. Information on JFCC-NW is limited, but according to USSTRATCOM public information, JFCC-NW plans and executes cyber attacks.[10] The JFCC-NW commander is currently dual-hatted as the Director of the NSA and is stationed at the home of the NSA, Fort Meade, Maryland. Additionally, the JFCC-NW deputy commander is also stationed at Fort Meade. By surface appearance, core CNE and CNA expertise is resident within NSA and some of that expertise is under the command or direction of USSTRATCOM. Although the Unified Command Plan (UCP) gives USSTRATCOM a cyberspace mission, it is not that of complete ownership of CNE or CNA. As joint doctrine reminds us, all combatant commands must coordinate, plan,

and execute information operations.[11] As multiple combatant commands are involved in CNE and CNA, there are a variety of organizational structures that support these missions.

CNA and CNE forces may be centrally organized together within one DoD office or they may be partly or wholly distributed within many DoD entities. Complete centralization of these specialists may occur in a defense agency, such as the NSA. These specialists would become the collectors of intelligence using cyberspace as well as the attack force. Whenever an analyst or operator requests intelligence, CNE would be just one of the disciplines, along with things like human intelligence (HUMINT) or SIGINT that may be used to answer the request. Similarly, when a combatant command requires CNA, this same organization would accomplish it. Alternatively, services and other agencies may field CNA forces or CNE forces or both. There are various advantages and disadvantages of these organizational approaches.

CNE and CNA forces should be organized together. To see this, consider a different scheme, where CNE and CNA forces are organized on their own. CNE operations are, in all likelihood, much more frequent than CNA operations in that we are constantly gathering intelligence on a wide variety of countries but we are actually conducting offensive operations in very few. Collecting information is a more benign and acceptable activity than conducting CNA. Because of this disparity in the amount of operations, CNE forces would become much more experienced than CNA forces at the core, common, ever changing intrusion techniques. CNA forces, like traditional military forces, would train at home station for assignment to a combatant command and employment in the field. While CNA forces can train on up-to-date cyber-ranges, in all

likelihood their expertise would be inferior to the real-world, tested skills of the separate CNE forces. Because of this disparity, the forces that perform CNE functions should also perform the CNA functions. While CNA and CNE should be organized together, they may also be centralized or distributed throughout the DoD.

CNA and CNE forces that primarily operate on the Internet or like networks should be centralized in a single DoD entity. In current practice, services are currently permitted to and have fielded cyber forces. The 2009 Quadrennial Roles and Missions Review Report states the DoD is "preserving Services' ability to field tactical [computer network operations] elements into their force structure."[12] The Air Force, for instance, has added cyberspace to its mission statement and has the 67th Network Warfare Wing with CND, CNE, and CNA missions.[13] However, as this field is in its infancy, the DoD has an opportunity to reduce duplication among the services. Giving one entity the CNA and CNE missions should not only reduce overall costs but should also increase the technical expertise of the forces due to the greater volume of work performed, simplify integration and synchronization of activities by not requiring the crossing of organizational boundaries, and improve the training of specialists due to common location and frequent interaction with other specialists. Finally, with only one entity as the force provider, combatant commands do not have to learn the nuances of different service capabilities to make the appropriate force or action request. While CNE and CNA forces should be centrally organized, defensive forces exist throughout the DoD.

Organization of Computer Network Defense Forces

Although all DoD personnel have a role in CND, certain DoD entities have much more significant roles than others. Defensive measures frequently result in trade-offs

where some capability is lost in the name of security. For example, consider Commander, USSTRATCOM's (CDRUSSTRATCOM) November 2008 DoD-wide ban of USB thumb drives on the NIPRNET.[14] The CDRUSSTRATCOM had to balance the risk of propagating malicious software through use of USB drives against their usefulness, such as easy loading of ever-present large Microsoft PowerPoint ® presentations in conference rooms. At least in the short term, CDRUSSTRATCOM determined that the risk DoD-wide was greater than the reward and subsequently banned their use. Key to these risk trade-off decisions is the scope and authority of the decision maker. Key decision makers include the SECDEF, the Chairman of the Joint Chiefs of Staff (CJCS), the CDRUSSTRATCOM, other combatant commanders, the Commander of JTF-GNO, the service chiefs of staff, and the directors of defense agencies.

At the top of the DoD policy and direction hierarchy is, of course, the SECDEF. Within the department is the dual-hatted Assistant Secretary of Defense for Networks and Information Integration and Chief Information Officer (ASD/NII). Both of these officials can issue policy and procedures regarding network defense. Since they are at the top of the DoD hierarchy, their policies affect the entire DoD. But there seem to be many more DoD-wide computer network operation and defense issues that need attention than the ASD/NII and SECDEF have the time or desire to address, so the SECDEF directed subordinates to handle this workload, the CDRUSSTRATCOM and the CJCS.

Per the UCP, USSTRATCOM directs operations and defense of DoD cyberspace. Similar to how it handles its other global missions, USSTRATCOM created

a subordinate organization to execute this mission, JTF-GNO. The Commander of JTF-GNO is also the Director of the Defense Information Systems Agency (DISA), the agency that manages long-haul network connections between military installations and also manages the connections between the NIPRNET and the Internet. As an example of JTF-GNO affecting global networks, leading up to the Feb 2008 shoot-down of the disabled U.S. spy satellite, JTF-GNO directed the suspension of network upgrades and maintenance (known as authorized service interruptions) to ensure such activity did not interfere with the shoot-down. As another example, network managers noticed the significant growth of recreational traffic on the NIPRNET. JTF-GNO raised the issue and led the effort to block YouTube and other sites on DoD networks. Just as the DoD has given DoD-wide cyber authorities to USSTRATCOM, it has also given authorities to the CJCS.

The CJCS, normally thought of as being involved with advice and doctrine, also has a role in CND policy. The CJCS may publish directives that apply to components of the DoD if he includes a reference to the appropriate authority to issue the directive.[15] In the case of CND, the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (a position that no longer exists) delegated authority to "develop and coordinate Joint [information assurance] policies and guidance" to the CJCS.[16] Based on this delegation, the CJCS issued instructions titled *Defense Information System Network (DISN): Policy and Responsibilities* and *Information Assurance (IA) and Computer Network Defense (CND),* among other computer related publications. While the CJCS and the CDRUSSTRATCOM have DoD-wide perspectives on CND, other combatant commands have narrower perspectives.

Like the DoD in general, the combatant commands have interests in defending friendly military cyberspace. Some friendly military cyberspace is well-contained within a geographic combatant command's area of responsibility (AOR) and consequently trade-off decisions are his responsibility. For example, a tactical data link network to build the friendly forces common operating picture in Iraq is within U.S. Central Command's (USCENTCOM) responsibilities, and trade-offs made in defending this network are properly made within USCENTCOM. Combatant commanders have this authority based on DoD Directive 5100.1, *Functions of the Department of Defense and Its Major Components,* which directs combatant command to employ forces and give authoritative direction to subordinate commands to perform assigned missions.[17] An example of a combatant command directing defensive measures is USCENTCOM's response to the recent concerns over USB thumb drive vulnerabilities. USCENTCOM decided to supplement the DoD solution for controlling USB ports on computers by purchasing and fielding additional software. Whereas combatant commands make use of capabilities like the above data link, Services, however, provide these capabilities.

Military Departments (MILDEPs) have significant roles in CND. MILDEPs "are responsible for, and have the authority necessary to conduct, all affairs of their respective Departments."[18] The MILDEPs are the entities that procure and operate most of the IT infrastructure, such as the many systems and networks on a base, post, camp, or station. As technology evolved over the years, the MILDEPs, in the absence of common DoD equipment and configurations, implemented defensive measures on their networks in different stages and in different ways. This has continued to the present, with predictable problems. For instance, the DISA bought and made freely available to

end users a DoD-wide chat and audio/video conferencing application. The Army and the Air Force updated their networks and made the application available to their users. However, the Navy noted a deficiency in the application's use of encryption and refused to implement. Despite the validity of the Navy finding, the other services continued to allow the application. The result was, for instance, that U.S., European Command (USEUCOM) action officers could use this application to hold web meetings with their components except for the Navy and that U.S. Pacific Command (USPACOM), which is on a Navy installation, could not use the application at all. In addition to the MILDEPs, there are defense agencies involved in network defense, such as the NSA and the DISA.

The NSA is a key organization when it comes to CND. It is responsible "for the security of national security information systems, covering the Department of Defense and other Federal departments and agencies."[19] In this capacity and related to CND, the NSA provides technical guidance, vulnerability analysis, and 24/7 threat warnings and attack alerts. Technical guidance includes things such as how to configure network equipment as well as configuration and use of recommended network security products. Although this technical guidance is extensive, the NSA has not assumed a directive role with respect to implementing this guidance. They leave it to other entities to make sound risk judgments based on the information provided. But the NSA is not the only defense agency with CND responsibilities. The DISA has many responsibilities as well.

Like the NSA, the DISA is also a key CND organization. DISA authority in this area is rooted in DoD Directive 8500.01E, *Information Assurance*, which directs the DISA Director to "develop, implement and oversee a single [information assurance]

approach" in coordination with the CJCS, the Defense Intelligence Agency, and the NSA.[20] Like the NSA, the DISA also develops technical configuration guidance and conducts 24/7 CND operations. The DISA has three Theater NetOps Centers (TNCs) with wide-area network management and defense responsibilities as well as one control and reporting TNC. TNC-Pacific is aligned with USPACOM and responsible for roughly the same AOR as USPACOM. TNC-Central Region (control and reporting only) is aligned with USCENTCOM. TNC-Europe is aligned with USEUCOM and U.S. Africa Command. TNC-CONUS is aligned with the other combatant commands. Day-to-day, these TNCs work with JTF-GNO and the combatant command J-6 staffs to operate and defend the network.

Given these multiple high-level entities with CND responsibilities, personnel have sought to clarify relationships using a model available in doctrine, that of "chain of command" based on *Doctrine for the Armed Forces of the United States*. This document, as well as the Unified Command Plan and the Forces for Unified Commands memorandum, describes two distinct chains of command, both beginning at the President to the SECDEF and then to either a combatant command or service secretary. The combatant commander chain is for "missions and forces assigned to their commands."[21] The MILDEP chain is "for purposes other than operational direction of forces assigned to the combatant commands."[22] As seen in the above example of the implementation of defense-wide collaboration tools on the NIPRNET, the MILDEP chain can cause inconsistencies in the network defense posture of the military. In that example, the Navy contended the system did not comply with a required encryption standard and refused to accept the risk and field it. The risk was if an adversary is able

to intercept communications between collaboration clients he may be able to, if necessary, decrypt them and then exploit them. Likewise, the combatant command chain of command can also cause inconsistencies in network defense posture, as shown by the USB flash drive ban. In this example, USCENTCOM fielded additional protective software that the services and other combatant commands did not. USCENTCOM determined the risk of only using the department-wide solution was too great and upgraded their defenses.

Entities having different CND postures raise issues of the joint concepts of unity of command and unity of effort. In some respects, the examples above clearly do not illustrate unity of command because forces under the same commander have different postures. For the collaboration example, Navy forces assigned to USPACOM could not use the tool but Army and Air Force forces assigned to USPACOM could. If unity of command was followed, an entity with DoD-wide authority would have either told the Army and Air Force to un-implement the system due to security risks or told the Navy to implement the system as the DoD accepts the risks. Similarly, in the second example a DoD-wide authority would have either told all the services, combatant commands, and agencies to implement the additional defensive measures or stopped USCENTCOM from “wasting” resources. However, the examples may illustrate unity of effort. According to doctrine, unity of effort is “coordination through cooperation and common interests [and] is an essential complement to unity of command.”[23] In the above examples, different DoD entities were all working towards the same common goal of information assurance. They achieved this goal with different actions and risk trade-offs, but they did make other organizations aware of their analysis and decisions. This

sharing of information so that all entities can make good decisions in pursuit of a common goal is an example of unity of effort.

Unity of command is currently depicted using C2 relationships between USSTRATCOM and components or between JTF-GNO and components. For example, Figure 1 shows organizations subordinated to JTF-GNO. Ignoring the distinction between a network operations and security center (NOSC) and a computer emergency response team (CERT) as it is not relevant to this paper, JTF-GNO has operational control (OPCON) and/or tactical control (TACON) of the service components. Other

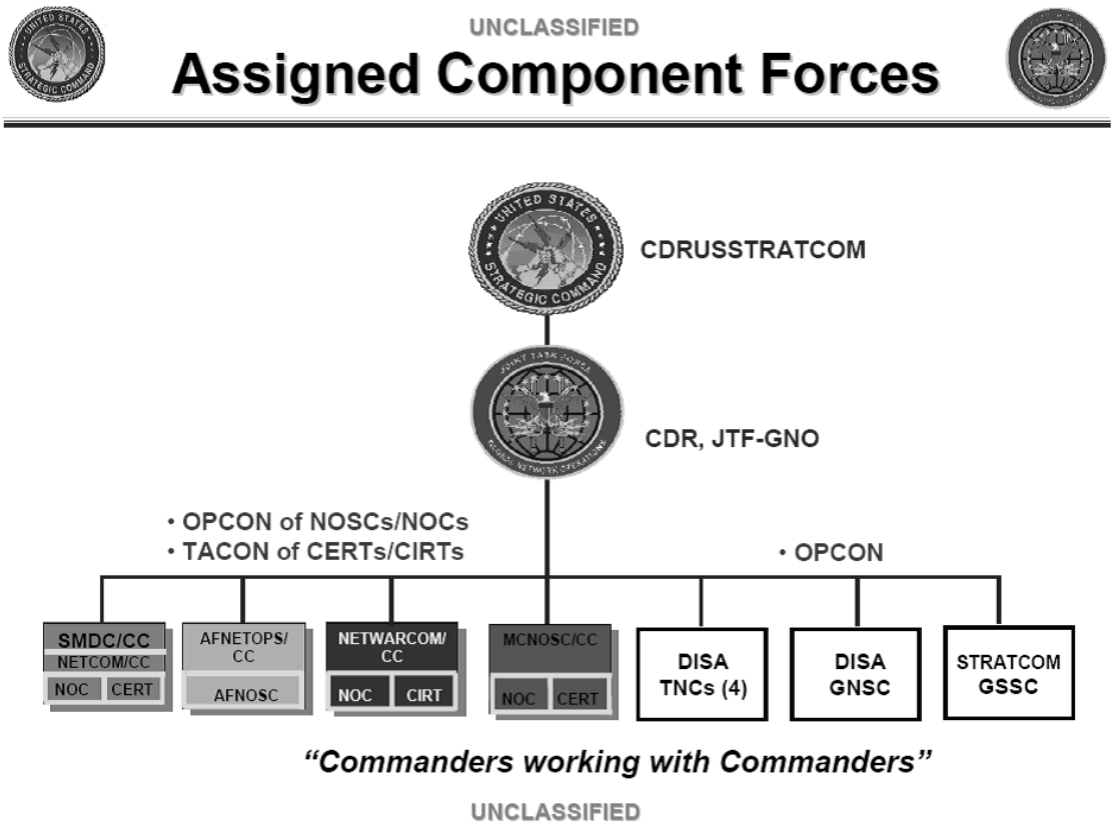

Figure 1: Forces Assigned to JTF-GNO[24]

DISA and USSTRATCOM entities are also OPCON to JTF-GNO. The service relationships are doctrinally sound and indicate that the classified memorandum Forces for Unified Commanders assigns services forces to USSTRATCOM and that USSTRATCOM has subsequently assigned OPCON or TACON to its subordinate JTF, JTF-GNO. Although this unity of command appears clear, the above examples raise questions. On one hand, the examples show a disjointed, unsynchronized DoD that one would hope unity of command would not permit. On the other hand, the examples show the differences among the MILDEPs, differences that are supported by United States Code Title 10, Armed Forces and the joint concept of administrative control (ADCON). While there are unity of command questions at the joint level, they also exist within the services.

Unity of command within the services is also depicted using C2 relationships. For instance, figure 2 shows Army Forces Strategic Command (ARSTRAT) as the Army component of USSTRATCOM and then an OPCON line from ARSTRAT to the Army Global NetOps and Security Center (AGNOSC) along with the text “AGNOSC is OPCON to STRATCOM thru ARSTRAT.” The Army component to USSTRATCOM is ARSTRAT, a three-star led Army Service Component Command (ASCC) that administratively reports to the Chief of Staff of the Army (CSA). However, the Army top-level organization with CND forces and responsibilities is Network Enterprise Technology Command (NETCOM), a two-star led unit that also reports to the CSA. ARSTRAT does not inherently possess the forces or authority to implement JTF-GNO CND orders Army-wide. NETCOM seemingly has that authority (more on that later) as well as some of the forces, specifically the AGNOSC. To solve this, the Commander of

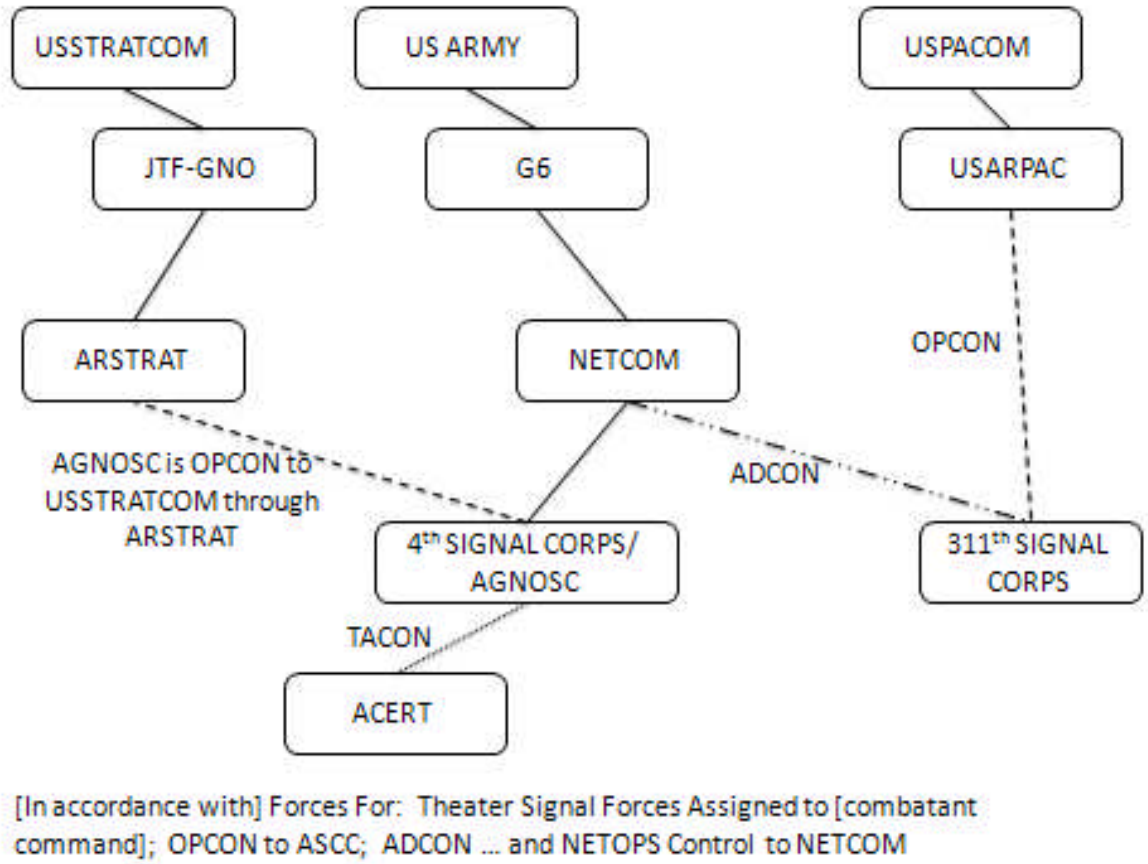

Figure 2: Army CND Command Relationships[25]

ARSTRAT delegates its CND mission to NETCOM, a relationship documented in an Army regulation.[26] Following this logic, NETCOM is a part of ARSTRAT and is therefore under the combatant command of STRATCOM. Further, STRATCOM can give OPCON of NETCOM to JTF-GNO. Just as the lines from JTF-GNO to the AGNOSC are at best complicated but clear, the lines from the AGNOSC to the rest of the Army are as well.

Figure 2 also shows how the Army achieves internal unity of command. It does this by saying "Theater Signal Forces [are] Assigned to [combatant command]; OPCON to ASCC; ADCON…and NETOPS Control to NETCOM."[27] The first relationship is doctrinally sound, the combatant command has combatant command authority

(COCOM) over theater assigned signal forces. The second relationship, theater signal forces are OPCON to ASCC, is also doctrinally sound; as these theater signal forces are assigned to the combatant command, he can delegate OPCON to his Army component which is known as an ASCC. The next relationship, theater signal forces are ADCON to NETCOM, is an Army-specific relationship that may be unfamiliar to other services. Outside of the Army and unlike this case, ADCON is often discussed when a force is OPCON to a different service, such as when a Marine force is OPCON to an Army joint force land component commander. Within the Army however, this relationship between functional headquarters, such as the signal headquarters, and field functional units is codified in an Army regulation that states ASCCs usually have ADCON of theater assigned Army forces but that certain units may also be ADCON to non-theater units.[28] Most novel to those outside the Army is the last relationship, "NETOPS control" between NETCOM and the theater signal forces. This relationship exists to give an avenue for direction from NETCOM to these field signal units even though they are OPCON to a different commander. Some Army documents refer to this as technical control (TECHCON). These complicated internal C2 relationships give rise to potential conflicts.

Because technicians can have multiple chains of command, with an ADCON chain and an OPCON chain for instance, they can receive conflicting orders. For instance, suppose an e-mail server is being operated by an Army signal unit assigned to USEUCOM. Suppose further that there is a new e-mail virus infecting DoD. Finally, suppose JTF-GNO, the Army, and USEUCOM come to different conclusions how to fight this virus, one directing the suspension of incoming/outgoing e-mail service and

another directing everyone to use Outlook Web Access instead of Outlook. In this fictional scenario, the technician's chain-of-command would have to sort out this conflicting guidance and determine which way they will implement. In practice, however, the nature of the incident determines who is in charge. For global incidents, JTF-GNO is in charge. For other incidents, geographic combatant commands or services may be in charge. In summary, in order to achieve unity of command in the CND realm, the DoD has created complicated relationships between joint force commanders and their components, complicated relationships within services, and complicated relationships between JFCs. Instead of this system, DoD could return to the root of the issue and simplify based on the authority of the SECDEF.

Whereas SECDEF has DoD-wide authority, SECDEF should delegate his CND authority to a new entity with CND responsibilities, the DoD Global Computer Network Operations Office. The manpower for JTF-GNO would be transferred to this office as a baseline. This action, although unusual, would eliminate the complicated C2 structures invented by the DoD to make the internal CND realm conform to combatant command doctrine. When this office releases direction to counter a vulnerability or thwart an attack, it does so with the authority of the SECDEF, not through a service component that does not truly have the forces or authority necessary to carry out the instructions. This office could be assigned to SECDEF, ASD/NII, USSTRATCOM, DISA, or even NSA, although the ultimate home for this office is of less importance than its actual existence. Services and agencies could follow suit and delegate CND authority from the service secretary to a service computer network operations office. Every CND directive

could contain a phrase like “Per DoD Directive X, this directive is issued on behalf of and with the authority of the SECDEF and therefore applies DoD wide.”

Clearly the DoD faces many challenges in the world of computer networks. As shown above, conducting CNE and CNA requires some of the same skills, being able to gain and maintain privileged access to adversary systems. Further, this access is enhanced by access to target networks, a core ability for the NSA to conduct its intelligence mission. Because of these factors, CNE and CNA should be centralized in the NSA. With respect to CND, there are multiple DoD entities with varying interests and this has led to complicated C2 structures. Realizing that CND authority emanates from the SECDEF, a simpler structure is to delegate his authority to a DoD entity and allow this entity to act on his behalf. These changes, should they be implemented, would continue DoD progress in cyberspace, allowing it to better protect U.S. security.

Endnotes

[1] Elaine Shannon, “The Invasion of the Chinese Cyberspies (And the Man Who Tried to Stop Them),” *Time*, August 29, 2005, http://www.time.com/time/magazine/article/0,9171,1098961,00.html (accessed February 28, 2009).

[2] *U.S. Department of Defense Dictionary of Military and Associated Terms,* http://www.dtic.mil/doctrine/jel/doddict/data/c/01461.html (accessed February 28, 2009).

[3] U.S. Strategic Command, “U.S. Strategic Command - Functional Components,” http://www.stratcom.mil/default.asp?page=functional_components, (accessed February 28, 2009).

[4] George W. Bush, *The National Strategy to Secure Cyberspace* (Washington DC: The White House, February 2003), ix, http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf (accessed February 28, 2009).

[5] U.S. Department of Homeland Security, “DHS | National Cybersecurity Division”, http://www.dhs.gov/xabout/structure/editorial_0839.shtm (accessed February 28, 2009).

[6] Bush, *National Strategy to Secure Cyberspace,* 17.

[7] The DoD also has a third role, critical infrastructure protection.

[8] Peter Pace, *The National Military Strategy for Cyberspace Operations* (Washington, DC: U.S. Joint Chiefs of Staff, 2006), 2, http://www.dod.mil/pubs/foi/ojcs/07-F-2105doc1.pdf (accessed February 28, 2009).

[9] Donna Miles, *New Unified Command Plan Spells Out Responsibilities, Missions* (Washington, DC: American Forces Press Service, December 23, 2008) http://www.defenselink.mil/news/newsarticle.aspx?id=52450 (accessed March 1, 2009).

[10] U.S. Strategic Command, "Functional Components."

[11] U.S. Joint Chiefs of Staff, *Information Operations,* Joint Publication 3-13 (Washington, DC: U.S. Joint Chiefs of Staff, February 13, 2006), xii, http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf (accessed March 2, 2009).

[12] Robert Gates, *Quadrennial Roles and Missions Review Report,* (Washington, DC: Secretary of Defense, January, 2009), 17, http://www.defenselink.mil/news/Jan2009/QRMFinalReport_v26Jan.pdf (accessed March 1, 2009).

[13] U.S. 8th Air Force, "8th Air Force – 67 NWW", http://www.8af.acc.af.mil/units/67nww/index.asp (accessed March 1, 2009).

[14] Bob Brewin, "Defense Bans Use of Removable Storage Devices," Nextgov.com, November 21, 2008, http://www.nextgov.com/nextgov/ng_20081121_2238.php (accessed March 1, 2009).

[15] U.S. Joint Chiefs of Staff, *Policy for the Development of CJCS, Joint Staff, and J-Directorate Directives*, Chairman of the Joint Chiefs of Staff Instruction 5701.01B (Washington, DC: U.S. Joint Chiefs of Staff, February 1, 2006), 1-2, www.dtic.mil/cjcs_directives/cdata/unlimit/5701_01.pdf (accessed March 1, 2009).

[16] U.S. Secretary of Defense, *Information Assurance (IA) Implementation,* U.S. DoD Instruction 8500.2 (Washington, DC: U.S. DoD, February 6, 2003), 3, http://www.dtic.mil/whs/directives/corres/pdf/850002p.pdf (accessed March 1, 2009).

[17] U.S. Secretary of Defense, *Functions of the Department of Defense and Its Major Components,* U.S. DoD Directive 5100.1 (Washington, DC: U.S. Secretary of Defense, August 1, 2002), 9, http://www.dtic.mil/whs/directives/corres/pdf/510001p.pdf (accessed March 1, 2009).

[18] Ibid, 11.

[19] U.S. National Security Agency, "Frequently Asked Questions about NSA - NSA/CSS," under "5. What is Information Assurance?" http://www.nsa.gov/about/faqs/about_nsa.shtml (accessed March 2, 2009).

[20] U.S. Secretary of Defense, *Information Assurance,* U.S. DoD Directive 8500.01E (Washington, DC: U.S. DoD, October 24, 2002), 8, http://www.dtic.mil/whs/directives/corres/pdf/850001p.pdf (accessed March 2, 2009).

[21] U.S. Joint Chiefs of Staff, *Doctrine for the Armed Forces of the United States*, Joint Publication 1 (Washington, DC: U.S. Joint Chiefs of Staff, May 14, 2007), II-4, http://www.dtic.mil/doctrine/jel/new_pubs/jp1.pdf (accessed March 2, 2009).

[22] Ibid.

[23] Ibid, IV-1.

[24] COL Carl Hunt, U.S. Strategic Command Director of Technology and Analysis, "Net-Centricity and Global NetOps" (lecture, Norfolk Waterside Marriott, Norfolk, VA, March 15, 2006), 9, http://www.dtic.mil/ndia/2006netcentric/hunt.pdf (accessed March 2, 2009).

[25] LTC Thomas Keller, U.S. Army Global NetOps and Security Center Chief of Current Operations, "Organizing for the NetOps Fight" (lecture, Broward County Convention Center, Ft. Lauderdale, FL, August 19, 2008), 6, http://www.afcea.org/events/pastevents/documents/Track4Session2.ppt (accessed March 2, 2009).

[26] U.S. Department of the Army, *Army Commands, Army Service Component Commands, and Direct Reporting Units,* Army Regulation 10-87 (Washington, DC: U.S. Department of the Army, October 4, 2007), 12, http://www.army.mil/usapa/epubs/pdf/r10_87.pdf (accessed March 2, 2009).

[27] Ibid.

[28] AR 10-87, 1-2.